# サーバプロテクションサービス 【管理者用】運用マニュアル

フルモデル(仮想パッチ+ウイルス対策)編

# 株式会社 大塚商会

Vol.SPS95 2017/12/01 1.2版

# はじめに

ここでは、本マニュアルについて説明します。

#### 対象読者

社内サーバ管理者、セキュリティ管理者

#### マニュアルの目的

本マニュアルは、サーバプロテクションサービスの機能および運用方法を理解していただくことを目的にしています。

#### マニュアル内の記述について

お客様がご使用になるOS環境により、表示・表現が本マニュアルと異なる場合がありますのでご了承ください。

\* Windows Server® 2003、Windows Server® 2008、Windows Server® 2012は、米国Microsoft Corporation の米国およびその他の国における登録商標または商標です。

\*Deep Securityは、トレンドマイクロ株式会社の登録商標です。

\*記載されている会社名および商品名は、各社の商標または登録商標です。なお、本文中では、<sup>※</sup>!やRなどの記号は使用しておりません。

\*記載されている商品名は特に断りがない限り日本語版です。

#### マニュアル内で使用している記号

略称	目的
ſ 」	マニュアルの名称を示します。
L T	ウィンドウの名称およびメッセージ、製品名、参照先を示します。
[ ]	メニューやタブの名称と、ボタンおよびキーを示します。
8	ウィンドウ、ダイアログ、コンソール画面などを示します。
8 E>F	操作および運用上のヒントを示します。
!重要	操作および運用上の注意を示します。
ЭМЕМО	操作および運用上の関連事項を示します。
<b>Ö</b> !!! []	マニュアル内、または別冊マニュアルの参照先を示します。

# 目次

1.サービスについて	3
1-1.基本用語	3
1-2.サービス内容	3
1-2-1.本サービスでご提供する内容	4
1-2-2.主なサービス概要	4
1-3.動作環境やご利用条件の概要	5
1-3-1.システム要件	5
1-3-2.ご利用条件	5
1-3-3.ご利用時の注意事項	5
2.お客様マイページについて	6
2-1.お知らせ	6
	7
2-3.お問い合わせ	
3.管理コンソールについて	10
3-1.ログオン	10
3-2.ログオフ	12
3-3.ダッシュボード	13
3-3-3.ウィジェットの配置変更	15
3-3-4.パスワードの変更	16
3-4.アラート、ログの参照	17
3-4-1.アラートの参照	17
3-4-2.不正プログラム対策イベントの参照	19
3-4-3. 侵入防御(仮想パッチ)イベントの参照	21
3-4-4.Web レピュテーションイベントの参照	23
3-5. サーバ情報の参照	25
3-6. レポート	27
3-6-1.レポート作成方法	28
3-6-2.(例)ウイルスレポート	32
3-6-3.(例) 侵入防御レポート	36
4.タスクトレイアイコンについて	40
	40
4-1.1 ハントリラ思	40
4-1-1.2フイアントの状態を確認する	40
4-1-2.ツフイ アントのイベントを確認 9 る	41
5.ウイルス <b>感染時</b> の対処方法	43
5-1 感染の確認	43
5-2.トレンドマイクロのホームページによるウイルス情報確認と削除	43
6.注意	45
6-1 管理コンパールのエラー表示	45
▼ 1:日·エー <i>ノ / / / / / 、</i> ス小 · · · · · · · · · · · · · · · · · ·	
7.その他	46
7-1.エージェントの追加	46
7-2 サーバのリプレース	46
7-3 設定の変更	46
	· · · TV

# 1.サービスについて

この章では、基本用語、機能、動作環境、導入から運用までの流れについて説明します。

## 1-1.基本用語

本サービスで使われる基本用語は、次の表のとおりです。

用語	脱明
マネージャー	対象サーバの管理と各種設定を保存するサーバです。
エージェントプログラム	対象サーバにインストールするプログラムです。
エージェント	本サービス管理下のサーバOSです。
管理コンソール	マネージャーに接続して、各種ログやレポートの表示を行うコンソールです。 Internet Explorerを使用します。
管理者ID	本サービス契約時に郵送した、管理コンソールへのログオンアカウントです。
侵入防御	パッチが適用されるまでの間、既知の脆弱性に対する様々な攻撃コードにさらされないようにします。 ※Deep Security 9.0 以降より、"Deep Packet Inspection"および"DPI"が"侵入防御"に名称変更されました。
仮想パッチ	ベンダーから正式なパッチが提供されるまでの一時的な対策として、仮想的に脆弱性を修正するプログラムです。
IPS	侵入防御システム。コンピュータへの不正な侵入の兆候を検知し、防御します。
Webレピュテーション	ウイルスに感染する危険性のあるWebサイトへの接続を自動的にブロックする機能です。

## 1-2.サービス内容

・仮想パッチ:トレンドマイクロ法人向け総合セキュリティソフト「Deep Security」の仮想パッチ(侵入防御)機能を ASP サービスとして提供します。

・ウイルス対策:トレンドマイクロ法人向け総合セキュリティソフト「Deep Security」の不正プログラムの駆除機能を ASP サービスとして提供します。

・お客様による管理サーバの設置・運用やライセンスの管理は不要で、エージェントとなるサーバ OS へのエージェントプログラムのインストールだけでご利用できます。



・管理コンソール:ログの参照やレポートの生成とダウンロードが可能です。

#### 1-2-1.本サービスでご提供する内容

本サービスでは以下のような環境をご提供します。

- ① インターネットブラウザーで閲覧するセキュリティ適用状況の確認画面(管理コンソール)
- ② 仮想パッチエージェントプログラム(Deep Security Agent)
- ③ ウイルス対策エージェントプログラム(Deep Security Agent)
- ④ 関連する各種マニュアル類一式
  - ※ ④関連する各種マニュアル類一式は、ご契約時にご案内するポータルサイトよりダウンロードできます。

#### 1-2-2.主なサービス概要

・仮想パッチ機能

OSの脆弱性を狙った攻撃に対し、その脆弱性を狙った攻撃コードを見分け、攻撃をブロックするために必要な仮想パッチを適用します。また、この 機能は弊社の推奨設定値にて定期的に脆弱性と適応済みセキュリティパッチをスキャンし、自動的に仮想パッチの適用・除去を行います。

・ウイルス対策機能

不正プログラムに対するリアルタイム検索及び予約検索を行います。不正プログラムを検出した場合は自動的に処理を行います。処理に失敗した場合は、別途手動での処理が必要です。また、エージェント側での手動検索は実行できません。

•Webレピュテーション

不正プログラムに感染する可能性が高いWebサイトへの接続制御を行います。不正プログラムに感染する可能性が高いWebサイトに接続しようとした場合は、ブロック画面が表示されます。

・ウィジェット

ウィジェットは管理コンソールのトップページに表示される情報パネルのことです。情報の種類を選択したり、レイアウトを変更したりすることが可能 です。

#### 参照 1 3.3.2ウィジェットの追加/割除

・サーバ情報の参照

エージェントとなっているサーバのOSや、管理のステータス、アップデートの状況などの情報を収集し、エージェントごとに閲覧できます。

参照 信 3.5サーバ情報の参照

・各種レポートの表示機能

本サービスでは、エージェントとなっているサーバOSでのDeepSecurity Agentの情報を収集し、各種レポートを表示します。 収集した情報をもとに、過去4週間分の仮想パッチによる攻撃防御や不正プログラムの検出状況などをレポートで確認できます。 ・アラートレポート ・不正プログラム対策レポート ・攻撃レポート ・侵入防御レポート ・概要レポート 他

参照 1 3.6レポート

## 1-3.動作環境やご利用条件の概要

#### 1-3-1.システム要件

対応 OS	Microsoft Windows Server 2012 R2(64 ビット)
	Microsoft Windows Server 2012(64 ビット)
	Microsoft Windows Server 2008 R2 (64 ビット)
	Microsoft Windows Server 2008(32 ビット/64 ビット)
	Microsoft Windows Server 2003 R2 SP2(32 ビット/64 ビット)
	Microsoft Windows Server 2003 SP2 (32 ビット/64 ビット)
仮想環境	Agent をインストールするゲスト OS がサポート対象であれば、ハイパーバイザー/ホストの種
	類に関わらずサポート対象。ただし、仮想環境のみで発生し物理環境で再現できない問題
	は、対応されない可能性があります。
メモリ	1GB(最小)、2GB(推奨)
HDD	500MB 以上のハードディスク空き容量
	(不正プログラム対策機能を使用する場合は1GB以上を推奨)
ネットワークプロトコルおよびサービス	TCP/IP、Microsoft Network、RPC サービスがインストール先サーバで実行されていること
	※記載のシステム要件は 2016 年 5 月現在のものです

#### 1-3-2.ご利用条件

以下、ご利用にあたっての注意事項の概略です。(詳しくは『ご利用条件』をご参照下さい。)

- 1.本サービスの開始に当たり、サーバへのインストールは弊社よりリモートで行います(初期費用が発生いたします)。弊社からのリモート接続ができない場合には、弊社エンジニアが作業を実施します。その際は別途有償となります。
- 2.リモート接続によるエージェントインストール作業は9:00~17:30の間に限られます。

3.エージェントソフトについて

- (1) ご提供する機能は仮想パッチとウイルス対策のみとなります。
- (2) ルールの割り当ては、推奨スキャン機能での提供となります。

・推奨スキャンは毎週木曜日、金曜日、土曜日、日曜日の0:00~8:00に実行します。(5:00~6:00の間はサーバ再起動のため、除く)

・該当の時間にサーバが停止していた場合は、次の推奨スキャンのタイミングに実行されます。

- (3) 緊急度の高い脆弱性ルールがリリースされた場合、事前の予告なく推奨スキャンを実行する場合があります。
- (4) 管理マネージャーからのレポート閲覧、レポート作成は、弊社が定めるサーバメンテナンス時間内は出来ません。
- (5) 管理マネージャーからのレポート閲覧、レポート作成は過去4週間分になります。
- (6) 他のウイルス対策ソフトとの同居は不可となります。本サービスのウイルス対策に乗り換える場合は、お客様自身でアンインストールして下さい。
- (7) サーバにエージェントをインストールする場合、ネットワークの一時的な切断、またはOSのネットワークドライバが他のプログラムによって使われている場合は、OSの再起動を求められる場合があります。
- (8) 以下の環境でDeep Security エージェントの動作はサポート対象外となります。

・Network Load Balanceを構成しているサーバ

- •Windows Server 2012 Server Core
- -Windows Server 2008 Server Core
- (9) エージェントソフトから直接インターネットへの443/TCP、4120/TCP、4122/TCPへアクセスが可能になっている必要があります。

#### 1-3-3.ご利用時の注意事項

- ※ 本サービスの実施により、セキュリティパッチの適応を不要とするものではありません。お客様で計画的にセキュリティパッチの適用を実施してい ただく必要があります。
- ※ 本サービスは、外部から不正アクセスやウイルスからの防御を完全にお約束するものではありません。ウイルス等の損害については、一切保証 致しません。導入後の状況は、お客様自身で管理画面からご確認ください。

# 2.お客様マイページについて

この章では、サーバプロテクションサービスのお客様マイページについて説明します。 お客様マイページでは、管理者様宛のお知らせのご確認や、マニュアルのダウンロードを行っていただくことができます。また、サーバプ ロテクションサービス管理コンソールへのログインもお客様マイページから行っていただきます。 お客様マイページのURL及びサーバプロテクションサービスのログイン用IDとパスワードは「サーバプロテクションサービス登録完了のお 知らせ」にも記載されておりますので、併せてご確認ください。

## 2-1.お知らせ

サーバプロテクションサービスに関するお知らせが発生した場合、お客様マイページから管理者様へお知らせいたします。「お知らせ」とは、メンテナ ンス情報、障害情報、誤検知情報、バージョンアップ情報等を指します。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。

<b>뽸大</b> 塚商会	▶ サポート ▶ フェア・セミナー ▶ お客様アンケート ▶ お問い合わせ ▶ English サイト内検索 検索
ホーム ソリューション・製品	品 お客様マイページ 通販(たのめーる) 企業情報
お客様マイページ 技術サポー トップ 情報を探	ート 問い合わせをする・ ソリューション・ 契約内容や マイページの 設定をする
ホーム > お客様マイページ > 技術サポー	▶情報を探す > 製品別・サービス会員ページ > サーバープロテクションサービス
<b> </b>	サーバープロテクションサービス
▲ 大塚ID 新規登録(無料) ・ 旧QQ-Webご利用のお客様へ	サーバプロディ 最新 2 件のお知らせが表示されます。確認したい件名のリンクをクリックします。 <sup>大塚商会がお3</sup> その他のお知らせを確認する場合は、「お知らせの一覧を見る」のリンクから一覧を表示し <sup>P</sup> 詳しいサー」認したい件名のリンクをクリックします。
<ul> <li>旧契約マイページご利用のお 客様へ</li> </ul>	お知らせ(最新2件)
<ul> <li>大塚IDとは</li> <li> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>2</sup> <sup>1</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>1</sup> <sup>2</sup> <sup>1</sup> <sup>2</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup> <sup>1</sup></li></ul>	2016年 6月10日 連結 ・ 【サーバープロテクションサービス】メンテナンスのお知らせ (2016年07月24日)
は添けポート特記を探す	2016年 4月14日 連絡 ・【サーパープロテクションサービス】メンテナンスのお知らせ (2016年05月07日)
	▶ お知らせの一覧を見る
よくあるご質問 (FAQ)	

② 「お知らせ」の詳細が掲示されているページが開きます。



# 2-2.各種手順書のダウンロード

管理者様向けの各種手順書はお客様マイページからダウンロードいただけます。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。



サーバプロテクションサービスについてご不明点がある場合、お問い合わせいただく窓口の情報をお客様マイページからご確認いただけます。

製品別・サービス会員ページ	メニュー		
サーバープロテクションサービス > 管理サイト(IDがSPSで始まるお 客様) 管理サイト(IDがDSNで始まるお	<ul> <li>管理サイト(IDがSPS で始まるお客様)</li> </ul>	管理サイト(IDがDSN で始まるお客様)	運用手順書(仮想パッ チモデル)
	□ 運用手順書(フルモデル)	■ 運用手順書(ウイルス 対策モデル)	アンインストール手順 書
動画で <del>サポ</del> ート 各種レポートダウンロード <mark>会</mark>	よくあるご質問(FA Q)	▶ お問い合わせ	
■ よくあるご質問 (FAQ)	▶ 製品別・サービス会員ページへ		
🛛 お知らせ		[お問い合わせ]を	クリックします。
お問い合わせ			Litima

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。

② ログイン画面が表示されます。 ※既にログイン済の場合は表示されません。

ログイン この機能を利用するには、ログインが必要です。

大塚IDでログインする場合は、大塚ID(メールアドレス)、パスワードを入力してください。 別のIDでログインする場合は、ログインするIDを選択してください。

大塚IDでログインする	別のIDでログインする	
大塚ID (メールアドレス)	会員番号 (旧QQ-WebのID) で ログイン	
例)abc@otsuka-shokai.co.jp	・ 旧222	
□次回からIDの入力を省略する パスワード & & & &	大塚 ID とパスワードを入力し[ログイン	]をクリックします。
	■個人IDとは	
▶ パスワードをお忘れですか?		
ログイン		

#### ③ お問合せフォームが表示されます。



お問い合わせ(サーバプロテクションサービス)

入力

#### ご依頼から対応までの流れ

受付フォームに内容をご記入下さい。自動で受信確認メールを返信いたします。 1. 2. 当社よりご希望の回答方法でご連絡いたします。

#### 1 注意爭項

- こちらのフォームに必要事項をご記入の上、送信してください。技術的なお問い合わせを申込 みいただけます。
- (必須)の部分は必ずご入力ください。
- お客様の保守契約内容・状況によりご回答できない場合がございます。予めご了承ください。
- サポート時間は月~金9:00~19:00となります。
- 誠に勝手ながら、受付日時や内容により、翌営業日の回答となる場合がございます。また、サ ポート時間外、当社休業日の場合は翌営業日の回答とさせていただきます。
- ファイルを添付できない場合は、ブラウザのアドオンを無効にしていただくと解決することが あります。

#### お問い合わせ内容

大塚ID	任意
会員番号	任意
会社名	<del>گاھ</del>

リモートサポート

大塚商会の連絡先

セキュリティ

クラウド・ASP

会員番号・パスワード再発行申し

コンタクトセンターの混雑状況を見

たよれーる 保守サポートのご紹介

大塚ID全般 お客様マイページ全般

込み

3

# 3.管理コンソールについて

この章では、サーバプロテクションサービスの管理コンソールについてご説明いたします。

# 3-1.ログオン

お客様マイページから、サーバプロテクションサービスの管理コンソールにログオンします。

① お客様マイページのURL(https://mypage.otsuka-shokai.co.jp/sps)へアクセスします。



① サーバプロテクションサービス管理コンソールのログオン画面が開きます。

	Security
ユーザ名:   パスワード: ログオン	
Copyright © 2014 Tre	ユーザ名とパスワードを入力し、[ログオン]をクリックします。 ユーザ名とパスワードは「サーバプロテクションサービス登録完了のお知らせ」で ご確認ください。



※次回以降表示不要の場合は、画面左下のチェックを外してください。

③ サーバプロテクションサービス管理コンソールが開き、ダッシュボード画面が表示されます。

TREND. Deep Security	,			SPS123456789 -	ログオフ   🔞 ヘルプ 🗸
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー		
Default     小       すべて ▼     24時間表示 ▼	VL1-9			٠	ウィジェットの追加削除
アラートステータス	× = 2K = -500 X	テータス コンピュータのステー ● 重大: ● 警告: ● 管理対象: ● 非管理対象:	× マイア タス: ユーザ: 1 0 0 泉彩ロ: 0 前回の 総ログ:	サウントのステータス × 名: <b>2</b> SPS123456789 1234567-株式会社o立or M1234567989(Role) ジオン: 2016-04-2014:03 ログオン: 2016-04-1916:16 オン回数: 6	ログオン属歴       ヘ         過去6回のログオン誌       2016-04-20 14         2016-04-20 14       2016-04-19 16         2016-04-18 14       2016-04-18 11         2016-04-18 11       2016-04-18 11
不正プログラム対策イベント履歴       ・ </td <td></td> <td><b>検索結果:</b> 駆除 原題 削除 放置 アクセン ■ 取除不</td> <td>× 不正ブ 感染コン 取得可 ス拒否 余</td> <td>ログラム対策のステータス (コンピュー ピュータのトップ5: 能な情報はありません 7</td> <td>タ) → <del>75-1</del> ■ (0) ■ (1)</td>		<b>検索結果:</b> 駆除 原題 削除 放置 アクセン ■ 取除不	× 不正ブ 感染コン 取得可 ス拒否 余	ログラム対策のステータス (コンピュー ピュータのトップ5: 能な情報はありません 7	タ) → <del>75-1</del> ■ (0) ■ (1)

サーバプロテクションサービス管理コンソールでの作業が終了したら、ログオフを行ってからブラウザを終了してください。

① サーバプロテクションサービス管理コンソールの右上にある[ログオフ]をクリックします。

	ep Security					SP S123456789	・  ログオフ   🕘 ヘルプ 🗸
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリ	37-		
Default     ⊕       すべて▼     248飛       アラートステータス		[	ログオフ]をクリ	ックしま	ंगे。		ウィジェットの追加剤除…
■ 重大: 1 最新のアラート: ■ 不正プログラム対策1	■ 警告: 期間 こンジンが… 1日	•	<b>コンピュータのステ</b> ~ ● 重大: ● 警告: ● 管理対象: ● 非管理対象:	-タス: 1 0 0	ユーザ名: 役割: 最終ロダオン: 前回のロダオン: 総ロダオン回数:	▲ SPS123456789 1234567-株式会社 △△□- M123456789(Role) 2016-04-20 14:03 2016-04-19 16:16 6	過去6回のログオン誌 2016-04-20 14 2016-04-19 16 2016-04-18 14 2016-04-18 11 2016-04-18 11
不正ブログラム対策イイ ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	ベント履歴		<b>検索結果:</b> ■ 駆除 ■ 隔離 ■ 削除 ■ 防隆 ■ アクセン ■ 転序体不	× ス拒否 (#)	不正プログラム決 感染コンピュータの 取得可能な情報は	十策のステータス (コンピュ トッブ5: ありません	一夕) ~ <b>〉</b>
(*)							アラート 🔤 (0) 📕 (1)

2 サーバプロテクションサービス管理コンソールのログオン画面に戻ります。

Deep Security	
ユーザ名:   パスワード:   ログオン	
Copyright © 2014 Trend Micro Inc. All rights reserved	

#### 3-3.ダッシュボード

ダッシュボードにはサーバプロテクションサービスで管理されているエージェントの情報が表示されます。

#### 3-3-1.ダッシュボードの概要

ダッシュボードでは、サーバプロテクションサービスで管理されているエージェントで発生しているイベントの概要やシステムの情報を確認することが できます。確認できる情報は以下の通りです。ただし、一部機能はサーバプロテクションサービスで提供しておりませんので、ご了承ください。

- 【サーバプロテクションサービスで提供している機能】
- ・アラートステータス
- ・アラート履歴
- ・コンピュータのステータス
- ・不正プログラム対策のステータス(コンピュータ)
- ・不正プログラム対策のステータス(不正プログラム)
- ・不正プログラム対策の保護ステータス
- 不正プログラム対策イベント履歴
- ・不正プログラム検索のステータス
- ・WebレピュテーションのURLアクティビティ
- ・Webレピュテーションのコンピュータのアクティビティ
- ・Webレピュテーションイベント履歴
- ・IPS IPのアクティビティ(検出)
- ・IPS IPのアクティビティ(防御)
- ・IPSのアクティビティ(検出)
- ・IPSのアクティビティ(防御)
- IPSイベント履歴
- ・IPSコンピュータのアクティビティ(検出)
- ・IPSコンピュータのアクティビティ(防御)
- ・アプリケーションの種類のアクティビティ(検出)
- ・アプリケーションの種類のアクティビティ(防御)
- ・アプリケーションの種類のツリーマップ(検出)
- ・アプリケーションの種類のツリーマップ(防御)
- ・最新のIPSのアクティビティ(検出)
- ・最新のIPSのアクティビティ(防御)
- ・システムイベント履歴
- ・マイアカウントのステータス
- ・ログオン履歴
- ・セキュリティアップデートのステータス

# 【サーバプロテクションサービスで提供していない機能】 ・ファイアウォールIPのアクティビティ(検出) ・ファイアウォールIPのアクティビティ(防御) ・ファイアウォールのアクティビティ(検出) ・ファイアウォールイベント履歴 ・ファイアウォールコンピュータのアクティビティ(検出) ・ファイアウォールコンピュータのアクティビティ(検出) ・ファイアウォールポートのアクティビティ(検出) ・ファイアウォールポートのアクティビティ(防御) ・攻撃の予兆検索のアクティビティ ・攻撃の予兆検索履歴 ・Managerノードのステータス ・アクティビティ概要

・ソフトウェアアップデート

#### 3-3-2.ウィジェットの追加/削除

ダッシュボードのウィジェットを追加、削除し、必要な情報を閲覧できるようにします。

① サーバプロテクションサービスのポータルサイトトップページを開きます。

Deep Security				SPS123456	789 -   ログオフ   🔞 ヘルプ -
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー		
Default     小       すべて マ     24時間表示 マ       マイユン       アラートステータス       重大:     1       酸告:       最新のアラート:       不正プログラ	ビュータ × コンピュータのス: 0 [ウィジェットの追加		× マイアカウ マイアカウ マイアカウ マイアカウ	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	<ul> <li>ウィジェットの追加剤(除</li> <li>エレグオン属歴 過去6回のログオン試</li> <li>2016-04-20 14</li> <li>2016-04-19 16</li> <li>2016-04-18 14</li> <li>2016-04-18 11</li> </ul>
不正プログラム対策イベント履歴       ・       ・       ・       く       <		<b>検索結果:</b> 嬰院 陽離 削除 政置 アクセス ■ 取水ない	× 不正 プログ 感染コンビ・ 取得可能な 数 現得可能な	ゔラム対策のステータス (コン ュータのトップ5: は情報はありません	■ 2016-04-18 11 ビュータ) アラート ■ (0) ■ (1)

ウィジェットの追加/削除の画面が開きます。

ウィジェットの追加削除	
<ul> <li>■ 監視</li> <li>■ Managerノードのステータス [3x1]</li> <li>■ アクティビティ概要</li> <li>■ アラートステータス</li> <li>■ アラートステータス</li> </ul>	必要な項目にチェックを入れ、不要な項目はチェックをはずしてください。
<ul> <li>□ コンピュータのステータス</li> <li>□ セキュリティアップデートのステータス</li> <li>□ システム</li> </ul>	
<ul> <li>□ システムイベント履歴 [2x1]</li> <li>☑ マイアカウントのステータス</li> <li>☑ ログオン履歴</li> </ul>	設定が出来ましたら、[OK]をクリックします。
<ul> <li>□ ホ正ブログラム対策</li> <li>✓ ホ正プログラム対策のステータス (コンピー)</li> </ul>	タ) V OK キャンセル

③ ダッシュボードで設定が反映されたことをご確認ください。

#### 3-3-3.ウィジェットの配置変更

① サーバプロテクションサービス管理コンソールが開き、ダッシュボード画面を表示します。



#### 2 ウィジェットが移動します。

Deep Security				SPS123456	789 -   ログオフ   🔞 ヘルプ -
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー		
Default         ⊕           すべて▼         24時間表示         マイコンピュー	-9				🛖 ウィジェットの追加削除
アラートステータス     ×       重大:     1     警告:     0       最新のアラート:     期間       ■ 不正ブログラム対策エンジンが     1日	マイアカウントのス ユーザ名: 役割: 最終ログオン: 前回のログオン: 総ログオン回数:	ステータス <b>2</b> SPS123456789 1234567-株式会社。△ M123456789(Role) 2016-04-20 14:03 2016-04-19 16:16 6	× ⊐×	(ユータのステータス コンピュータのステー ● 重大: ● 管告: ● 管理対象: ● 非管理対象:	× ログオン属歴 へ タス: 1 0 0 0 0 2016-04-20 14 2016-04-19 16 2016-04-18 11 2016-04-18 11 2016-04-18 11
不正プログラム対策イベント履歴       4       そ       く		<b>検索結果:</b>	× 不正: 感染= 取得: 拒否 *	ブログラム対策のステータス (コン ュンピュータのトップ5: 可能な情報はありません	ビュータ) <b>アラート</b> (0) (1)

#### 3-3-4.パスワードの変更

「サーバプロテクションサービス登録完了のお知らせ」に記載されているパスワードは初期パスワードとなっておりますので、お客様にて変更をお願い いたします。また、発行後のパスワードに関してはお客様管理とさせていただきますのでお忘れにならないようお願いいたします。

① サーバプロテクションサービスの管理コンソールにログオンします。

Deep Security				SPS123456789 - ログオフ   🥝 ヘルブ -
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー	ユーザブロパティ
Default 中 すべて▼ 24特闘表示 ▼ マイコンビュー	\$		Y 7:4	→ ウィジェットの追加削除
エテ: 「ログオン名」-「/	ペイノカシンのの	ミクリックします	•	「パスワードの変更」を選択します。
	最終ログオン: 201 前回のログオン: 201 総ログオン回数: 6	6-04-20 14:03 6-04-19 16:16		● 警告: 0 2016-04-19 16 ● 管理対象: 0 2016-04-18 14 ● 非管理対象: 0 2016-04-18 11 ■ 2016-04-18 11
不正プログラム対策イベント履歴			× 不正プログラムネ	対策のステータス (コンピュータ)
4×+		検索結果:       駆除       駆除       削除       放置       アクセス指	※来コノビュータ0. 取得可能な情報は	かっつつ: 切りません

#### ② 現在のパスワード・新しいパスワード/確認入力にそれぞれ入力をします。

バスワード設定	
ユーザ: 現在のパスワード: 新しいパスワード: 新しいパスワードの確認入力: ごのシステムのパスワードの条件は次のとおりです: ・8文字以上であること ・英字と数字の両方が含まれていること 0K キャンセル	「現在のパスワード」、「新しいパスワード」、「新しいパスワードの確認入力」 に入力してください。



## 3-4.アラート、ログの参照

管理コンソールから各エージェントの状態を確認します。運用時に確認するべき項目は以下のとおりです。最低でも週に一度、定期的に確認を行うようにしてください。

- ・アラート
- ・ 不正プログラム対策イベント
- ・ 侵入防御イベント
- ・ Webレピュテーションイベント

#### 3-4-1.アラートの参照

管理コンソールの[アラート]からエージェントで発生しているアラートを確認します。 アラートとは、各エージェントでパターンファイルが更新されていない、検索エンジンがオフラインになっている等、何らかの問題が発生した場合に、 管理コンソール上に通知を出す機能です。

#### ① サーバプロテクションサービスの管理コンソールにログオンします。



#### 2 アラートの画面が表示されます。

	ecurity				SPS123456789 ▼   ログオフ   🥝 ヘルプ ▼
ダッシュボード ア	ラート	イベントとレポート	コンピュータ	ポリシー	
アラート 概要ビュー マ 時間	別 👻				🌆 アラートの設定
コンピュータ: マイコンピュータ		~			•
1台で不正プログラム対策エンジン1	がオフライン	ೇಕ			時刻: 2016-04-19 12:05
Agent/Applianceが、不正プログラ. マ 詳細の表示	ム対策エンシ	ジンが応答していないことをレ	ボートしました。コンビュ・	ータのシステムイベントを	6確認して、失敗の原因を特定してください。
			[詳細の表	長示]をクリックし	ます。
«					アラート 🔤 (0) 📕 (1)

#### ③ アラートの詳細が表示されますので、内容をご確認ください。

	ecurity				SPS123456789 ▼   ログオフ   @ ヘルプ ▼
ダッシュボード ア	クラート	イベントとレポート	コンピュータ	ポリシー	
アラート 概要ビュー マ 時間	踢↓ ▼				🌆 アラートの設定
コンピュータ: マイコンピュータ		~			•
1台で不正プログラム対策エンジン	がオフラインで	.च			時刻: 2016-04-19 12:05
Agent/Applianceが、不正プログラ.	み対策エンジ	ンが応答していないことをレ	ポートしました。 コンビュー	-タのシステムイベン	トを確認して、失敗の原因を特定してください。
▲ 詳細非表示					
<b>時刻:</b> 2016-04-	-19 12:05				
前回のアップデート: 2016-04-	-19 12:05				
<b>重要度:</b> 重大					
コンピュータ: 📃 serve	/er 不正力	コグラム対策エンジンがオフ	ライン		
*					

●MEMO 主なアラートの種類		
主なアラートには以下のような種類があります。		
アラート名	重要度	内容
侵入防御エンジンがオフライン	重大	侵入防御エンジンが認識できません。
Relayアップデートサービスを利用不可	重大	アップデートサーバに接続できません。この場合、トレンドマイクロ社のア ップデートサーバからアップデートを行います。
Webレピュテーションイベントアラート	警告	エージェントでWebレピュテーションのポリシー違反等のイベントが発生し ています。
不正プログラム対策コンポーネントのアップデートの 失敗	重大	ウイルスパターンファイル等、コンポーネントのアップデートに失敗してい ます。
コンピュータがアップデートを受信していない	警告	サーバプロテクションサービスのサーバから各エージェントに出されたア ップデートの通知を、エージェントが受信していません。
コンピュータの再起動が必要	警告	エージェントがインストールされている端末でOS再起動が必要です。
不正プログラム対策アラート	警告	ウイルスが検出されています。
不正プログラム対策エンジンがオフライン	重大	不正プログラム対策エンジンが認識できません。
新しいパターンファイルアップデートがダウンロード済 みで利用可能	警告	サーバプロテクションサービスのサーバが新しいパターンファイルまたは エンジンを取得し、利用可能な状態になっています。

#### 3-4-2.不正プログラム対策イベントの参照

管理コンソールの[不正プログラム対策イベント]から各エージェントでウイルス感染していないかを確認します。[不正プログラム対策イベント]とは、 ウイルスやスパイウェアに感染した際に発生するイベントです。

① サーバプロテクションサービスの管理コンソールにログオンします。



#### ② 不正プログラム対策イベントの画面が表示されます。

Deep Securit	ty			-
ダッシュボード アラート	[イベント	]-[不正プロク	ブラム対策イベント]をクリックします	
E 📑 イベント	₩174774	- 11	100001 ▼	<b>_</b>
	<sup>地会</sup> 通去7日間			
日 💽 千正フロクラム対象イベンド 🔞 隔離ファイル	コンピュータ: マイコンピュータ	•		
📟 Webレビュテーションイベント	🔄 表示 🚯 エクスポート 🗸 🧳	自動タグ付け…	[]] 列	
圆 ファイアウォールイベント	時刻 🔻	コンピュータ	感染ファイル	9 <u>7</u>
◎ 侵入防御イベント	× 🗋 2016-04-25 15:24:38	server	C:¥Users¥Administrator¥AppData¥Local¥Microsoft¥Windows¥…	
◎ 変更監視イベント	2016-04-25 13:54:10	server	C:¥Users¥Administrator¥AppData¥Local¥Microsoft¥Windows¥…	
● セキュリティログ監視イベント	2016-04-25 13:54:10	server	C:¥Users¥Administrator¥AppData¥Local¥Microsoft¥Windows¥···	
■ レポートの生成	2016-04-25 13:40:11		C:¥Users¥Administrator¥AppData¥Local¥Microsoft¥Windows¥···	
	2016-04-25 13:40:08			
	2016-04-25 13: 2016-04-25 13: 2016-04-25 13:	詳細の	確認をしたい[イベント]をダブルクリックします	0
«			フラート 🔤 (1)	(0)

#### ③ イベントの詳細が表示されますので、内容をご確認の上、適宜ご対応ください。

<b>一般</b> タグ	]
一般情報	
コンピュータ:	server
送信元:	Agent
不正プログラム情報	報
検出時刻:	2016-04-25 15:24:38
不正プログラム:	Eicar_test_file
感染ファイル:	C:¥Users¥Administrator¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.IE5 ¥GHWASSD.¥eicar[1].com
検索の種類:	UTNALA
検索結果:	削除
理由:	1234567-株式会社oooo-M123456789-server01(リアルタイム検索)
主要なウイルスの	種類: ウイルス

MEMO ウイルス感染時の対処方法

「検索結果」に表示される処理が「駆除」、「削除」、「隔離」以外の場合、別途ウイルスの処理を行う必要があります。

**診照** 13 5.ウイルス感染時の対処方法

# アビント 不正プログラム対策イベントを表示する期間の指定

不正プログラム対策イベントは、初期値では過去1時間のイベント表示する設定になっています。期間は「過去1時間」、「過去24時間」、「過 去7日間」と、「カスタム範囲」があります。カスタム範囲を選択した場合は、開始と終了の日時を設定し、右側にある矢印をクリックします。

不正プログラム対策イベント	すべて ▼ グループ化し	talı 👻	Q 検索	•
期間: 過去1時間 過去24時間 コンピュータ: 過去7日間 力スタム範囲:		-		•
		<b>T</b> -1		

|==|表示|| ▶| エクスボート → | 24 目動タク付け... 日間 列...

不正プログラ	ラム対策イベント	すべて▼ グループ化しない ▼	Q 検索	-
期間:	カスタム範囲:	~		
	開始: 2016-04-01	14:25	終了: 2016-05-01 🗰 15:25 ⊘	♦
コンビュータ:	マイエンビュータ	$\checkmark$		
<u></u> == ±=	<b>ポ</b> コ エクフポート	🔎 白釉为岩(井) 💷 제		

#### 3-4-3. 侵入防御(仮想パッチ)イベントの参照

管理コンソールの[侵入防御イベント]から各エージェントで仮想パッチに関連するイベントが発生していないかを確認します。[侵入防御イベント]とは、 推奨スキャンで適用された仮想パッチに対して攻撃が行われた場合に発生するイベントです。

#### ① サーバプロテクションサービスの管理コンソールにログオンします。

Deep Security				SP S123456789 <del>~</del>	ログオフ   🕜 ヘルプ 🕶
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー		
Default     ①       すべて ▼     24時間表示 ▼       マイコンビュン       アラートステータス       エ大:     1       警告:     0       最新のアラート:     期間       不正プログラム対策エンジンが     1 日	-タ -タ -タ -タ -タ -タ -タ - - - - タ - - - - - - - - - - - - -	:部のメニューに 2016-04-20 14:03 2016-04-19 16:16 6	-ある[イベントと	- - - - - - - - - - - - - -	<ul> <li>ウィジェットの追加哨!!味…</li> <li>/履歴</li> <li>のログオン試</li> <li>016-04-20 14</li> <li>2016-04-19 16</li> <li>2016-04-18 14</li> <li>2016-04-18 11</li> <li>2016-04-18 11</li> </ul>
不正プログラム対策イベント履歴       イ、       イ、       く		<b>検索結果</b> : 動除 周離 削除 放置 アクセス ・	× 不正フロ: 感染コンゼ 取得可能が れた否 #*	ダラム対策のステータス (コンピュー ュータのトップ5: な情報はありません	-5)

#### 2 侵入防御イベントの画面が表示されます。

	p Security				SPS1234	<b>56789 -  </b> 미성	ジオフ 🛛 🔞 ヘルプ 🕶
ダッシュボード	7 <del>5</del> -ŀ	イベントとレポート	コンピュータ	ポリシー			
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	ŧ	[イベ	ント]-[侵入防御	イベント]をクリックしま	₹ <b>†</b>		•
💮 Webレビュテーショ:	21~21	<u></u> □エクスポート	<ul> <li></li></ul>	🌆 列			
	~~2h	時刻 🕶	コンピュータ	アプリケーションの種類	処理	重要度	理由
🞯 侵入防御イベント		2016-04-25 15:25:29	server	Web Client Common	リセット	ф	DPI動作確認
● え史監視1ヘノト	**	2016-04-25 15:25:29	server	Web Client Common	リセット	中	DPI 動作確認)
● セキュリティログ監察	現イベント 🔤	2016-04-25 15:25:29	server	Web Client Common	リセット	中	DPI 動作確認)
10日本 一下の生成		2016-04-25 15:25:29		Web Client Common	リセット	中	DPI 動作確認)
		2016-04-25 15:25:29		Foot Common	リセット	中	DPI動作確認
		2016-04-25 15:25 2016-04-25 15:25 2016-04-25 15:25 2016-04-25 15:25 2016-04-25 15:25		細の確認をしたい[イ	ベント]をタ	「ブルクリッ	っします。
	C	0018 04 36 16:30	CONIOF	Web Client Common	i i dan da	÷	DDI 新小在政策习I
«						75-	ት 📃 (1) 📕 (0)

#### ③ イベントの詳細が表示されますので、内容をご確認ください。

→般 タグ				
┌一般情報───				
時刻:	2016-04-25 15:25:29			
コンピュータ:	server			
イベント送信元:	Agent			
理由:	DPI動作確認用ルール			
処理:	リセット			
方向:	送信			
70-:	接続フロー			
ランク:	25 = 資産評価 × 重要度 = 1 × 25			
インタフェース:				
「バケットの種類-				
プロトコル:	ТСР			
フラグ:	ACK PSH DF=1			
-₩₫				
IP:	192 168			
MAC:				
ポート:	55845			
└ 送信牛				
	124			
MAC				
ポート:	80			
「パケットデーター				
パケットサイズ	1204			
<戻る	次へ > 閉じる			

# ●MEMO 侵入防御イベント発生時の対処方法

特定の端末に侵入防御イベントが大量に発生している場合は、外部から攻撃を受けている可能性があります。弊社エンジニアまでご相談ください。

侵入防御イベントは、初期値では過去1時間のイベント表示する設定になっています。期間は「過去1時間」、「過去24時間」、「過去7日間」と、 「カスタム範囲」があります。カスタム範囲を選択した場合は、開始と終了の日時を設定し、右側にある矢印をクリックします。

不正プログラ	<b>ラム対策イベント</b> すべて ▼ グループ化	:Utal) 👻	<b>へ</b> 検索	-
期間:	過去1時間 過去24時間			
コンピュータ:	過去7日間 カスタム範囲:			

□□ 表示 ● エクスホート → 20 自動327回け… 日間列…

不正プログ	ラム対策イベント	すべて▼ グループ化しない ▼	٩	検索		-
期間:	カスタム範囲: 開始: 2016-04-01	14:25	終了: 2016-05-01	15:25	Ø	•
コンピュータ:	マイエンビュータ	~				
<u></u> == ±=	d□ τクフポート	🔎 白 わなどけけ 🛛 🖽 別				

#### 3-4-4.Webレピュテーションイベントの参照

管理コンソールの[Webレピュテーションイベント]から各エージェントでウイルス感染する危険のあるWebサイトに接続していないかを確認します。

#### ① サーバプロテクションサービスの管理コンソールにログオンします。

Deep Security		_		SPS1234567	789 🗸   ログオフ   🔞 ヘルプ 🗸
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー		
Default     -       すべて ▼     24時間表示 ▼       マイコンビュー       アラートステータス	3				ウィジェットの追加有耶念
<ul> <li>重大: 1 ■ 警告: 0</li> <li>最新のアラート: 期間</li> <li>■ 不正プログラム対策エンジンが 1日</li> </ul>	最終ログオン: 2 前回のログオン: 2 総ログオン回数: (	上部のメニュー 2016-04-20 14:03 2016-04-19 16:16 5		レポート]をクリック 0 a a: ● 管理対象: ● 非管理対象:	Cます。 0 2016-04-18 14 2016-04-18 11 2016-04-18 11
不正ブログラム対策イベント履歴 ・ 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、		<b>検索結果:</b> 駆除 原題 消防 放置 アクセス の 単応を示す	<ul> <li>× 不正ブログラ 感染コンピュー</li> <li>取得可能な情</li> <li>指否</li> </ul>	ラム対策のステータス (コン) -タのトップ5: 報知はありません	ピュータ)
					> アラート □ (0) ■ (1)

② Webレピュテーションイベントの画面が表示されます。

Deep S	ecurity	,		SPS12345678	9 -   ログオフ   🔞 ヘルプ -
ダッシュボード 7	᠈ᡔ᠆ᡰ	[イベント]	- [Web レピュ	ェテーションイベント]をクリックしま	ŧ <b>す</b> 。
🗉 🏬 イベント					
□ システムイベント	с.њ	期間:	~	•	
		コンビュータ: マイエンビュータ	~	1	
💭 Webレビュテーションイベ	52F	📰 表示 🛛 エクスポート 👻 🧐	🕘 自動タグ付け	[]]] 列	
○ ファイアウォールイベント ○ 得み 8±約 くべつよ		時刻 🔻	コンビュータ	URL	9 <u>7</u>
		2016-04-25 15:23:56	server	http://wrs41.winshipway.com/	
● 変更監視イベント	***	2016-04-25 13:40:50	server	http://wrs41.winshipway.com/favicon.ico	
でもして マンティロク 監視1 へ		2016-04-25 13:40:50	server	http://wrs41.winshipway.com/	
しホートの生成		2016-04-25 13:40:49	.or	http://wrs41.winshipway.com/	
		2016-04-25 13:40:49		http://wrs41.winshipway.com/favicon.ico	
		2016-04			
		2016-04	詳細の確認	をしたい[イベント]をダブルクリッ	クします。
		2016-04			
		2016-04			
	ſ	2016 04 25 12-40-42	conjor	http://www.f1.winchinwov.com/	>
«					アラート 🔤 (1) 📕 (0)

#### ③ イベントの詳細が表示されますので、内容をご確認ください。

_ <b>─般</b> ≶	<del>ت</del>			
┌一般情報──				
時刻:	2016-04-25 13:40:50			
コンピュータ:	server			
送信元:	Agent			
URL: http://wrs41.winshipway.com/favicon.ico				
	再評価			
ランク:	100 = 資産評価×重要度 = 1 × 100			
リスク:	危険			
< 戻る	次へ> 閉じる			

## WEMO Webレピュテーションイベントの対処方法

特定の端末でエンドユーザ様に覚えのないWebサイトへのアクセスがブロックされたイベントが発生している場合は、その端末がウイルス感染し ている可能性があります。調査をご要望の場合は弊社担当エンジニアまでご連絡ください。

# ジビント Webレビュテーションイベントを表示する期間の指定

Webレピュテーションイベントは、初期値では過去1時間のイベント表示する設定になっています。期間は「過去1時間」、「過去24時間」、「過 去7日間」と、「カスタム範囲」があります。カスタム範囲を選択した場合は、開始と終了の日時を設定し、右側にある矢印をクリックします。

不正プログラ	ラム対策イベント	<b>すべて</b> ▼ グループ化しない	<b>~</b>	<b>Q</b> 検索	•	
期間:	過去1時間 過去24時間					
コンピュータ:	過去7日間 力スタム範囲:					
	51102#~	2 自動交流111 🔠 列				

不正プログ	ラム対策イベント	<b>すべて</b> ▼ グループ化しない ▼	<b>Q</b> 検索	-
期間:	カスタム範囲:	~		
	開始: 2016-04-01	14:25 📀	終了: 2016-05-01 🏢 15:25 ⊘	►
コンピュータ	: マイエンビュータ	~		
±	<u>「</u> 」 ナクフポート	🔊 白 釉力岩(井) + 🛄 제		

## 3-5. サーバ情報の参照

エージェントになっているサーバOSの情報を管理コンソールから参照することができます。

#### ① サーバプロテクションサービスの管理コンソールにログオンします。



2 サーバプロテクションサービスで管理されているエージェントが表示されます。OSや各機能のステータスはこちらから確認可能です。



コンピュータ: server			0	ヘルプ
■ 概要				
😨 不正プログラム対策				^
📟 Webレビュテーション	ホスト名: 	server	(前回使用式わた)P:	
🛞 ファイアウォール	表示名:			
侵入防御	I.兑8月:			
変更監視     変更監視				
セキュリティログ監視	プラットフォーム:	Microsoft Windows Server 2008 R2 (64 bit) Service Pack 1 Build 7601		
🥮 インタフェース	グループ:	コンビュータ 🕨 推奨SCAN(土)1-2 🕨 1234567-M123456789 🛛 💌	]	
💮 設定	ポリシー:	1234567-株式会社0000-M123456789-server01(フルモデル) 💌	編集	
	資産の重要度:	tal 🔽	編集	
	│ セキュリティアップデートのダウンロード │ 元:	初期設定のRelayグループ	編集	
	「ステータスーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー			1
	Agent			
	ステータス: 😑 管理対象 (ス	オンライン)		
	不正プログラム対策: 🎧 オン,リアル	314		
	Webレビュテーション: 🎧 オン			
	ファイアウォール: 💮 オフ, インス	トールされています, ルールなし		
		444 ルール		
	②更監視: ● ライセンス許     ○ ライセンス許     ○ ライセンス許     ○ - イン・ラーン			
	セキュリティロク監視: (1) フイセンス計	+•)/a/U		~
	LI 477472. 1910			
			保存開じる	

項目名	アイコン	状態	意味
ステータス	管理対象(オンライ)		サーバプロテクションサービスの管理対象で、管理サーバとオン ライン状態です。正常時はこちらの状態になります。
	Θ	管理対象(オフライン)	サーバプロテクションサービスの管理対象で、管理サーバとオフ ライン状態です。
			※オフラインであってもアイコンの状態はオンラインと同じです。 必ず状態の表記をご確認ください。
不正プログラム対策	<b>(</b>	オン、リアルタイム	不正プログラム対策がオンの状態です。
_			サーバプロテクションサービスの「フルモデル」または「ウイルス 対策モデル」をご契約戴いたお客様はこの状態になります。
	6	オフ、インストールされ ていません	不正プログラム対策がオフの状態です。
			サーバプロテクションサービスの「仮想パッチモデル」をご契約戴 いたお客様はこの状態になります。
Webレピュテーション		オン	Webレピュテーションがオンの状態です。
			サーバプロテクションサービスの「フルモデル」または「ウイルス 対策モデル」をご契約戴いたお客様はこの状態になります。
	オフ、インストール ていません	オフ、インストールされ	Webレピュテーションがオフ状態です。
		ていません	サーバプロテクションサービスの「仮想パッチモデル」をご契約戴 いたお客様はこの状態になります。
侵入防御		防御、XXルール	侵入防御がオンの状態で、XXは有効なルール数を表していま す。
			サーバプロテクションサービスの「フルモデル」または「仮想パッ チモデル」をご契約戴いたお客様はこの状態になります。
	GEN	オフ、インストールされ	侵入防御がオフの状態です。
		ていません	サーバプロテクションサービスの「ウイルス対策モデル」をご契約 戴いたお客様はこの状態になります。

※ファイアウォール機能はサーバプロテクションサービスでは提供しておりません。

表示は「オフ、インストールされています、ルールなし」で問題ありません。

管理コンソールから生成できるレポートについてご説明します。

サーバプロテクションサービスの管理コンソールから確認いただける主なレポートの種類は以下の通りです。

レポートはPDF形式かリッチテキスト方式のいずれかで生成することができます。

なお、レポートの対象とすることができる期間は、レポート生成時から過去4週間分の情報のみとなりますので、ご了承ください。

レポート名	説明
アラートレポート	指定した期間中のアラートを「頻度別の種類」、「時系列」でレポートします。
不正プログラム対策レポート	指定した期間中の「不正プログラムに感染したコンピュータのトップ25」、「不正プログラムのトップ25」、「未完了の予約 検索」をレポートします。
コンピュータレポート	「コンピュータのステータス」、「OSの種類」、「前回のアップデート」情報などがレポートされます。
侵入防御レポート	指定した期間中の「侵入防御イベントの履歴(防御モード、検出モード)」、各モード毎の「イベントトップ25」「送信元IPト ップ25」、「アプリケーション種類のトップ25」をレポートします。
推奨設定レポート	推奨スキャンにより推奨設定された「アプリケーションの種類」や「侵入防御ルール」をレポートします。
<b>概要レポート</b>	指定した期間中の「アラートのトップ5」、「感染のトップ5」、「Webレピュテーションのトップ5」およびアラートレポート、不 正プログラム対策レポート、Webレピュテーションレポートなどの簡易情報をまとめてレポートします。
Webレピュテーションレポート	指定した期間中の「Webレピュテーションイベントのトップ25」、「URLのトップ25」をレポートします。

# とントレポート生成の条件

レポートを生成する際、条件を設定することが可能です。レポートによって、設定できる条件とできない条件があります。 詳細は以下の一覧をご確認ください。

#### 【主なレポートの条件】

レポート名	形式	期間	コンピュータ	暗号化
アラートレポート		•過去24時間		
		•過去7日間		—
		・カスタム範囲		
不正プログラム対策レポート		•過去24時間		
		•過去7日間		—
	_	・カスタム範囲		
コンピュータレポート		_	・マイコンピュータ	_
侵入防御レポート	PDF または	•過去24時間	・グループ内のコンピュータ ・セキュリティプロファイルを使用	
		•過去7日間		—
	97774AP	・カスタム範囲	しているコンピュータ	
推奨設定レポート		_	・コンピュータ名指定	_
概要レポート		・過去24時間		
		•過去7日間		—
		・カスタム範囲		
Webレピュテーションレポート		・過去24時間		
		•過去7日間		—
		・カスタム範囲		

#### 3-6-1.レポート作成方法

① サーバプロテクションサービスの管理コンソールにログオンします。

Deep Security		_		SPS123456789 ▼   ログオフ   🔞 ヘルプ ▼
ダッシュボード <b>アラート</b>	イベントとレポート	コンピュータ	ポリシー	
Default				
すべて▼     24時間表示▼     マイコン       アラートステータス	ピュータ × マイアカウン	上部のメ	ニューにある	5 <mark>[イベントとレポート]をクリックします。</mark>
<ul> <li>重大: 1 ■ 警告: 最新のアラート: 期間</li> <li>■ 不正プログラム対策エンジンが 1日</li> </ul>	<ol> <li>ユーザ名: 役割: 最終ログオン: 前回のログオン: 総ログオン回数:</li> </ol>	L SPS1234567-耕式会社。△ 1234567-耕式会社。△ M123456789(Role) 2016-04-20 14:03 2016-04-19 16:16 6		エンビュータのステータス:     ● 重大:     ● 管理対象:     ● 非管理対象:     ●     非管理対象:     ●
不正プログラム対策イベント履歴		<b>検索結果:</b> ■ 駆除 ■ 隔離 ■ 削除 ● 放置 ■ アクセス ■ 町称本:#	× 不正づ 感染コ 取得可 拒否	ログラム対策のステータス (コンピュータ) ンピュータのトップ5: "能な情報はありません 、
<ul> <li>(*)</li> </ul>				アラート 🔤 (0) 🔳 (1)

#### レポートの画面が表示されます。

Deep Security	,	SPS123456789 ▼   ログオフ   @ ヘルプ ▼
ダッシュボード アラート	イベントとレポート <b>エンビュータ ポリシー</b>	
<ul> <li>□ □ イベント</li> <li>□ システムイベント</li> <li>□ システムイベント</li> <li>□ ○ 不正ブログラム対策イベント</li> <li>◎ □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○</li></ul>	レポートの生成 単独レポート レポート: レポートの選択 形式: ダイ	
● セキュリティロ分覧視イベント ■ レポートの生成	【イベント】 - [レポートの生成]をクリ:	ックします。
	<ul> <li>期間</li> <li>● 過去24時間</li> <li>● 過去7日間</li> <li>● 前月(2016年3月)</li> <li>● カスタム範囲: 開始: 2016-04-21 Ⅲ 13:40 </li> </ul>	~
≪ 図 1台のエンピュータでセキュリティア	ップデートを実行中	アラート 🔤 (0) 🔳 (1)

#### ③ レポートの形式を選択します。

	p Security	,			SPS123456789 +   ログオフ   🔞 ヘルプ	*
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー		
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	策イベント aンイベント (ペント – 親イベント –	レポートの生成 単独レポート レポート: 侵入財 形式: 水ータ リッチ タヴ ・ すべて: ・ タヴなし ・ タヴなし ・ タヴ:	御レポート ブルドキュ父トフォーマ デキスト形式(RTF) [レポート]の: また、[	✓ ット (PDF) プルダウンから 形式]から生成	5、生成したいレポートの種類を選択します。 なしたいレポートの種類を選択します。	^
<ul> <li>(≪) 図 1台のエンビュー</li> </ul>	ダでセキュリティア	<ul> <li>○ 過去7日間</li> <li>○ 前月 (2016年3月)</li> <li>○ 前月 (2016年3月)</li> <li>○ カスタム範囲: 開約</li> <li>ッブデートを実行中</li> </ul>	2016-04-21	13:40	⊘ ▽ラート ■ (0) ■ (1)	~

#### ④ タグの設定をします。

TREND. Deep Securit	у			SPS123456789 ▼   ログオフ   🛞 ヘルプ ▼
ダッシュボード ア <del>フ</del> ート	イベントとレポート	コンピュータ	ポリシー	
<ul> <li>■ イベント</li> <li>■ システムイベント</li> <li>■ システムイベント</li> <li>■ マージョンゴント</li> <li>● 「協範ファイル</li> <li>● Webレビュテーションイベント</li> <li>※ ファイアウォールイベント</li> <li>※ ファイアウォールイベント</li> <li>※ 受見入防御イベント</li> <li>● 変更監視イベント</li> <li>● 変更監視イベント</li> <li>● セキュリティログ監視イベント</li> <li>● レポートの生成</li> </ul>	レポートの生成         単独レポート         レポート:         パート:         ダグ:         リート:         クラウない:         タグ:         リート:         リート:         パート:         クラウない:         リーン:         リーン:         パート:         リーン:         パート:         パート:         リーン:         パート:         リーン:         リーン: </th <th>抑レポート ジルドキュメントフォーマ</th> <th>'까누 (PDF) V</th> <th></th>	抑レポート ジルドキュメントフォーマ	'까누 (PDF) V	
(«)				アラート 🔤 (0) 🔲 (1)

# 8 E21 37

イベントデータを含むレポートを選択する場合、イベントタグでレポートをフィルタするオプションを使用できます。[すべて]は全てのイベント、 [タグなし]はタグ付けされていないイベントを対象とします。また、[タグ]を選択して1つ以上のタグを指定すると、指定したタグを含むイベント のみをレポートに含めることができます。 ※本サービスではタグはご利用できません。

#### 5 期間を指定します。

Deep Securit	y	SP\$123456789 ▼   ログオフ   @ ヘルブ ▼
ダッシュボード アラート	イベントとレポート	<b>ゴル・コータ ポリドノー</b>
<ul> <li>□ □ イベント</li> <li>□ システムイベント</li> <li>□ ② 不正プログラム対策イベント</li> <li>○ 福麗ファイル</li> <li>○ WebLビュテーションイベント</li> </ul>	レポートの生成 単独レポート ○ タヴなし: ○ タヴ・	[過去 24 時間]か[過去 7 日間]を選択します。 [カスタム期間]を選択した場合は期間を指定します。 ただし、4 週間以上以前の日時を指定しても、情報は含まれませんので、ご了承ください。
<ul> <li>※ ファイアウォールイベント</li> <li>※ 侵入防御イベント</li> <li>※ 変更監視イベント</li> <li>※ 支更監視イベント</li> <li>※ セキュリティログ監視イベント</li> <li>▶ レポートの生成</li> </ul>	<ul> <li>○ カナ.</li> <li>● 過去24時間</li> <li>● 過去7日間</li> <li>● 前月 (2016年3月)</li> <li>● カスタム範囲: 開始: 終7:</li> </ul>	
«		

#### ⑥ コンピュータを指定します。

TREND. Deep Security	y		SPS123456789 -   ログオフ   🔞 ヘルブ -
ダッシュボード アラート	イベントとレポート		#1187-
	レポートの生成		[マイコンピュータ]を選択してください。
■ ● ● ホエフロフラスネスネイ・シド (編稿) (編稿) (一) (編)(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)		2010-04-21	
<ul> <li></li></ul>	<ul> <li>● マイゴンピュータ</li> <li>○ グループ:</li> </ul>	コンピュータ ロサブグループ持会める	
▶ レポートの生成	○ 使用ポリシー:	なし ロサブボリシーも含める	· · · · · · · · · · · · · · · · · · ·
	○ コンピュータ: 「暗号化	コンピュータ名	
	● レポートのパスワート	"の無効化	

#### ⑦ 暗号化の設定をします。

	Security	/				SPS123456789 ▼   ログオフ   (	② ヘルプ ▼
ダッシュボード	7 <del>5</del> -ŀ	イベントとレポート	コンピュータ	ポリシー			
E 📑 イベント		レポートの生成					
<ul> <li>システムイベント</li> <li>⑦ 不正プログラム対策イ</li> </ul>	ベント	単独レポート	日日ゴガルニーは合める				
で つういい で で いってい いってい いってい いってい いってい いってい いって	イベント	○ 使用ポリシー:	はし ロージャント 2015			<b>v</b>	^
<ul> <li>         ・ ファイアウォールイベン</li></ul>	/h _	0 コンピュータ:	■サフボリシーも含める server		$\checkmark$		
	<	暗号化					
しポートの生成		<ul> <li>● レポートのパスリード</li> <li>● 現在のユーザのレボ・</li> </ul>	の無効化 -トのバスワードを使用				
		<ul> <li>カスタムレポートのパ、 パスワードの確認入す</li> </ul>	スワードの使用:				
						生成	~
«						アラート 🔤 (0)	) 🔲 (1)

Deep Secur	ity			SPS123456789 -   ログオフ   😧 ヘルプ -
ダッシュボード アラート	イベントとレポート	コンピュータ	ポリシー	
	レボートの生成			
	単独レポート	■サブグループも含める		
● № 00000000000000000000000000000000000	○ 使用ポリシー: た	au   +:		
────────────────────────────────────	〇 コンピュータ: st	erver パスワ	フードの使用を有す -	効にした場合は、パスワードを設定してください。 
<ul> <li>         ・ 変更監視イベント         ・         ・         ・</li></ul>	─ 「暗号化 · · · · · · · · · · · · · · · · · · ·	無効化		
🔣 レポートの生成	● 現在のユーザのレポート	のバスワーム使用		
	パスワードの確認入力:	•••	•••••	
				生成
«				アラート 🔤 (0) 📕 (1)

#### ⑧ 設定が終わったら、レポートを生成します。

	o Security	1		<b>SPS123456789 ▼</b>   ログオフ   @ ヘルプ ▼	
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー	
🗉 🧱 イベント		レポートの生成			
📃 システムイベント 🗉 🧒 不正プログラム対策	きイベント	単独レポート	■ サブグループも含め?	5	
「福福ファイル   Mebレビュテーション	مار <sup>س</sup> مر.	○ 使用ポリシー:	なし	-	~
<ul> <li>         ・ ファイアウォールイイ         ・         ・         ・</li></ul>	×C		[生成]をクリッ	クします。	
<ul> <li>マセキュリティログ監約</li> <li>レポートの生成</li> </ul>	見イベント	<ul> <li>レポートのパスワードの</li> <li>ロボートのパスワードの</li> </ul>			
		<ul> <li>○ 現在のユーリのしホー</li> <li>○ カスタムレポートのパス</li> </ul>	マードの使用:		
		バスワードの確認入力	:		
					生成
«					アラート 🔤 (0) 🔲 (1)

#### ⑨ レポートが生成されます。

sps2.tayoreru.com から 推奨設定	レポートpdf (75.9 KB)を聞くか、または(保存しますか? × 
L	レポートが生成されるとダウンロードの画面が表示されますので
	任意のフォルダに保存してください。

#### 3-6-2.(例)ウイルスレポート

例として、不正プログラム対策レポートの生成手順を記載いたします。

#### ① サーバプロテクションサービスの管理コンソールにログオンします。

	p Security	,	_		SP\$123456789 -	コグオフ 🛛 🔞 ヘルプ 🕶
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー		
Default 4						
すべて ▼ 24時間表示 アラートステータス	<b>⊼ ▼</b>   ⊽1⊐:	ンピュータ × マイアカウン	上部のメ	ニューにある	」[イベントとレポート]をクリック	します。
■ 重大: 1 日 最新のアラート: ■ 不正プログラム対策エ	<mark> 警告:</mark> 期間 ンジンが 2日	<ol> <li>ユーザ名: 役割: 最終ログオン: 前回のログオン: 総ログオン回数:</li> </ol>	▲ SPS123456789 1234567-株式会社⇔2 M123456789(Role) 2016-04-21 15:15 2016-04-21 14:21 9	-02	<ul> <li>二とピュータのステータス:</li> <li>●重大: 1</li> <li>●警告: 0</li> <li>●管理対象: 0</li> <li>● 非管理対象: 0</li> </ul>	2016-04-21 1 2016-04-21 1 2016-04-21 1 2016-04-20 1 2016-04-20 1 2016-04-19 1
不正プログラム対策イイ	いた履歴		<b>検索結果:</b> ■ RFR金	× 不正ブ 感染コ	ログラム対策のステータス (コンピュータ ンピュータのトップ5:	)
🤘 📝 1台のゴンビュー	タでセキュリティア	ップデートを実行中			75	·나 🔤 (0) 📕 (1)

#### ② レポートの画面が表示されます。

Deep Securit	ty			SPS123456789 ▼   □	ゴジオフ   @ ヘルプ マ
ダッシュボード ア <del>ラ</del> ート	イベントとレポート	コンピュータ	ポリシー		
<ul> <li>マステムイベント</li> <li>システムイベント</li> <li>システムイベント</li> <li>マボブログラム対策イベント</li> <li>隔離ファイル</li> <li>Webしどュテーションイベント</li> <li>ファイアウォールイベント</li> <li>クス防御イベント</li> <li>変更監視イベント</li> <li>文更監視イベント</li> <li>セキュリティログ転退イベント</li> </ul>	レポートの生成 単独レポート レポート:レポー 形式:	トの選択	✓ [イベント] - [レポ-	ートの生成]をクリックしま	
<ul> <li>レポートの生成</li> <li> </li> <li> </li> <li></li></ul>	<ul> <li>● タラオ</li> <li>● タグ:</li> <li>● タグ:</li> <li>● 過去24時間</li> <li>● 過去7日間</li> <li>● 過去7日間</li> </ul>		÷	79	~-+ (0) (1)

#### ③ レポートの形式を選択します。

#### ④ レポートのファイル形式を選択します。

Deep Securit	ty	SP\$123456789 -   ロジオフ   🥡 ヘルプ -
ダッシュボード アラート	イベントとレポート <b>コピュ</b>	A #16
<ul> <li>■ 1ベント</li> <li>■ システムイベント</li> </ul>	レポートの生成	ここでは用途に合わせてファイル形式を選択します。
<ul> <li>○ イエニフレクラム対策イベント</li> <li>「福蔵ファイル</li> <li>● Webレビュテーションイベント</li> <li>● ファイアウォールイベント</li> <li>○ 侵入防御イベント</li> </ul>	レポート レポート:不正ブログラム対策し 形式: <u>ホータブルドキュックト</u> リッチテキスト形式 (R	* -ト ▼ 7# -マット (PDF) TF)
<ul> <li>変更監視イベント</li> <li>セキュリティログ監視イベント</li> <li>レポートの生成</li> </ul>	<b>タグ</b> ● すべて: ○ タヴねし: ○ タヴ:	-f-
		¥
« 📝 1台のコンピュータでセキュリティ	アップデートを実行中	アラート 🔤 (0) 📕 (1)

#### ⑤ タグの設定をします。

ダッシュボード アラート				
	イベントとレボート	コンピュータ	ポリシー	
<ul> <li></li></ul>	レポートの生成			
<ul> <li>□ システムイベント</li> <li>□ マ 不正 プログラム対策イベント</li> <li>○ 不正 プログラム対策イベント</li> <li>○ 陽石 アーションイベント</li> <li>○ ファイアウォールイベント</li> <li>○ 侵入防御イベント</li> <li>○ 変更監視イベント</li> </ul>	<ul> <li>単独レポート</li> <li>タヴ</li> <li>・ すべて:</li> <li>・ タヴねし:</li> <li>・ タダなし:</li> </ul>			^ ^
<ul> <li>セキュリティログ監視イベント</li> <li>レポートの生成</li> </ul>	- <b>期間</b> ● 過去24時間 ○ 過去7日間			[すべて]を指定します。
	○前月 (2016年3月)			

#### ⑥ 期間を指定します。

	Security	,			<b>SPS123456789 -</b> │ ログオ	フ   @ ヘルプ マ
ダッシュボード	ア∋ート	イベントとレポート	コンピュータ	ポリシー		
<ul> <li>ボック・シント</li> <li>システムイベント</li> </ul>		レポートの生成				
E ② 不正プログラム対策 「福雄ファイル	イベント			5		
●●● Webレビュテーション ●● ファイアウォールイベ ●● オッチング	バベント ベント	<ul> <li>期間</li> <li>● 過去24時間</li> <li>● 過去24時間</li> </ul>				
<ul> <li></li></ul>	-	○ 過去7日間 ○ 前月(2016年3月)				
🔣 レポートの生成			L.			
				[過去 24 時間]を	選択します。	
( 🛛 1台のユンビュータ	でセキュリティア	ップデートを実行中			75-1	_ (0) 📕 (1)

#### ⑦ コンピュータを指定します。

	ep Security				SPS123456789 ▼   ログオフ
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー	
<ul> <li>□ □ □ イベント</li> <li>□ システムイベント</li> </ul>		レポートの生成			
□ ⑦ 不正ブログラム対	) 第イベント ョンイベント イベント ──	」単独レボート       _			^
<ul> <li></li></ul>	1. 「「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、	<ul> <li>● マイエンピュータ</li> <li>○ グループ:</li> </ul>	14		<b>v</b>
▶ レポートの生成		01	[マ	イコンピュータ	]を選択します。
		『暗号化			~
ĸ 🔯 1台のエンビュー	・タでセキュリティア・	ップデートを実行中			アラート 🔤 (0) 🔲 (1)

#### ⑧ 暗号化の設定をします。

	ep Security				SPS123456789 ▼   ログオフ   @ ヘルプ ▼
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー	
E 🔚 イベント		レポートの生成			
<ul> <li>□ システムイベント</li> <li>□ ⑦ 不正プログラム対</li> <li>○ 福雄ファイル</li> </ul>	策イベント	<b>単独レポート</b> 〇 コンピュータ:		[レポートノ	ペスワードの無効化]を選択します。
● WebL2ュアーン: ◎ ファイアウォールイ ② 侵入防御イベント ● 変更監視イベント ③ セキュリティログ整 ■ レポートの生成	■ノイベント イベント 	<ul> <li>暗号化</li> <li>● レポートのパスワード()</li> <li>● 現在のユーザのレル</li> <li>○ カスタムレポートのパン パスワードの確認入力</li> </ul>	の無効化   - のパスワートを使用 スワードの使用: []:		
					生成 マラート - (0) - (1)

#### ⑨ 設定が終わったら、レポートを生成します。

TREND Deep Secur	ity			SPS123456789 🕶 🛛 ログオフ 🗎 🔞 ヘルプ 🕶
ダッシュボード アラート	イベントとレポート	コンピュータ	ポリシー	
🗉 🧱 イベント	レポートの生成			
<ul> <li>システムイベント</li> <li>マ 不正プログラム対策イベント</li> </ul>	単独レポート	サゴボルシーを分める		
「福雄ファイル   Mableピュテーションイベント	0 コンピュータ:	・9 シホッシー 0 3 0 3 ンピュータ名		×
<ul> <li>◎ ファイアウォールイペン</li> <li>◎ 侵入防御イベント</li> <li>◎ 変更監視イベント</li> </ul>		[生成]をクリッ	クします。	
③ セキュリティログ監視イベント	<ul> <li>カスタムレポートのパスワ パスワードの確認入力:</li> </ul>	ワードの使用:		

#### 10 レポートが生成されます。

sps2.tayoreru.com から 不正プログラム対策レポート.pdf(	×	
	• キャンセル(C)	
	レポートが生成されるとダウンロート 任意のフォルダに保	<sup>、</sup> の画面が表示されますので、 存してください。

#### 3-6-3.(例)侵入防御レポート

例として、仮想パッチのレポートである侵入防御レポートの生成手順を記載いたします。

#### ① サーバプロテクションサービスの管理コンソールにログオンします。

	ep Security	,			SPS123456789 ▼ □	コグオフ 🛛 🕜 ヘルプ 🗸
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー		
Default 🕂						
すべて▼ 24時間表: アラートステータス	<b>⊼ ▼</b>	ンピュータ × マイアカウン	上部のメ	ニューにある	[イベントとレポート]をクリック	します。
<ul> <li>重大: 1</li> <li>最新のアラート:</li> <li>■ 不正プログラム対策エ</li> </ul>	<mark>- 警告:</mark> 期間 :ンジンが 2日	<ol> <li>ユーザ名: 役割: 最終ログオン: 前回のログオン: 総ログオン回数:</li> </ol>	▲ SPS123456789 1234567-株式会社⇒2 M123456789(Role) 2016-04-21 15:15 2016-04-21 14:21 9	-22	<ul> <li>ユレビュータのステータス:</li> <li>● 重大: 1</li> <li>● 警告: 0</li> <li>● 管告: 0</li> <li>● 管理対象: 0</li> <li>● 非管理対象: 0</li> </ul>	2016-04-21 1 2016-04-21 1 2016-04-21 1 2016-04-20 1 2016-04-20 1 2016-04-19 1
不正プログラム対策イイ	ベント履歴		<b>検索結果:</b> ■ BTCR金	× 不正ブ 感染コ:	ログラム対策のステータス (コンピュータ) ンピュータのトップ5:	~
< 📝 1台のコンピュー	タでセキュリティア	ップデートを実行中			77	~F 🔤 (0) 📕 (1)

#### ② レポートの画面が表示されます。

TREND. Deep Sec	curity			SPS123456789 ▼   ログオフ   @ ヘルプ ▼
ダッシュボード アラ	- <b>h</b> イベントとレ	ポート <b>ゴンビュータ</b>	ポリシー	
<ul> <li>□ □ イベント</li> <li>□ システムイベント</li> <li>□ システムイベント</li> <li>□ アモブログラム対策イベント</li> <li>③ 不正ブログラム対策イベント</li> <li>③ ア・アウォールイベント</li> <li>③ ② ファイアウォールイベント</li> <li>③ ② 三、「「「「「」」」</li> </ul>		ート: <mark>レポートの選択</mark> :	マ [イベント] - [レフ	ポートの生成]をクリックします。
<ul> <li>         ■ 00 - 00 ± 8x     </li> </ul>	<ul> <li>● 35%</li>     &lt;</ul>	9	c <sup>r</sup> u <sup>2</sup>	7∋−ト ■(0) ■ (1)

#### ③ レポートの形式を選択します。

Deep Securit	y			SPS123456789 -   ログオフ   🔞 ヘルブ -	
ダッシュボード アラート	イベントとレポート	コンピュータ	ポリシー		
E	レポートの生成				
<ul> <li>         システムイベント     </li> <li>         図 不正プログラム対策イベント     </li> </ul>	単独レポート	_		ミュー (1月11日) (11日) (111)	
<ul> <li>(福 隔離ファイル)</li> <li>(1) Webレビュテーションイベント</li> <li>(2) ファイブウェール くびいし</li> </ul>		<b>1</b>	(	℃は[使人防御レ小━٢]を選択しまり。	
<ul> <li>◎ ファイアリオールイヘンド</li> <li>◎ 侵入防御イベント</li> <li>◎ 変更監視イベント</li> </ul>		ログラム対策レポート ポート Ile Recommendation			
<ul> <li>セキュリティログ監視イベント</li> <li>レポートの生成</li> </ul>	● すべて: コンピュ コンピュ コンピュ コンピュ	ウォールレボート - ータフォレンジックフ - ータレポート			
	○ タグ: (侵入防 推奨該 概要レジ	御レポート 走レポート ポート			
		アブリケーション活動しオ ムイベントレポート ビュテーションレポ <i>ー</i> ト	<-⊦ -	· · · · · · · · · · · · · · · · · · ·	
<ul> <li>«</li> </ul>				アラート 🔤 (0) 🔲 (1)	

#### ④ レポートのファイル形式を選択します。

Deep Security	,	SPS123456789 マ   ログオフ   @ ヘルプ マ
ダッシュボード アラート ● ● イベント ● システムイベント ● マ 不正プログラム対策イベント ● マ 不正プログラム対策イベント ● マ 不正プログラム対策イベント ● マ アイアウォールイベント ● ファイアウォールイベント ● マ マ ト	イベントセレポート     エンピ:       レポートの生成     ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ここでは用途に合わせてファイル形式を選択します。
<ul> <li>● えと面除す・マーゴ</li> <li>● セキュリティログ監視イベント</li> <li>● レポートの生成</li> </ul>	<ul> <li>すべて:</li> <li>タガなし:</li> <li>タガ:</li> </ul>	- - - - - - - - - - - - - - - - - - -

⑤ タグの設定をします。

	o Security	,			SPS123456789 ▼   ログオフ   🔞 ヘルプ ▼
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー	
		レポートの生成			
<ul> <li>⇒ システムイベント</li> <li>○ 不正プログラム対策</li> <li>○ 福道ファイル</li> <li>○ Webレビュテーション</li> <li>○ ファイアウォールイベ</li> <li>○ 侵入防御イベント</li> <li>○ 家事転換イベント</li> </ul>	:1~2)t 21~2)t ~2)t ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	単独レポート ・ ダグ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・			~
<ul> <li>で、セキュリティログ監約</li> <li>・レポートの生成</li> </ul>	린イベント	● 過去24時間 ● 過去24時間 ● 過去7日間 ● 前月(2016年3月)			[すべて]を指定します。
«					アラート 🔤 (0) 📕 (1)

#### ⑥ 期間を指定します。

	p Security			SP S1	123456789 -   ログオフ   @ ヘルプ -
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー	
<ul> <li>日 読 イベント</li> <li>システムイベント</li> <li>ロ ジステムイベント</li> <li>ロ ジ 不正ブログラム対象</li> <li>(福麗ファイル</li> <li>○ Webレビュテーション</li> <li>③ ファイアウォールイイ</li> <li>② 侵入防御イベント</li> <li>③ 変更監視イベント</li> <li>③ 変更監視イベント</li> <li>③ 支更監視イベント</li> <li>③ セキュリティログ監約</li> <li>○ レポートの生成</li> </ul>	そイベント ンイベント ペント ~ 見イベント	レポートの生成 単独レポート ・ ジッ・ ジッ・ ジッ・ ジッ・ ジッ・ ジッ・ ジッ・ ジッ・		で 14.33 [過去 24 時間]を選択しまで	
	?でセキュリティア	ップデートを実行中			アラート 🔤 (0) 🔲 (1)

#### ⑦ コンピュータを指定します。

	ep Security				SPS123456789 ▼   ログオフ
ダッシュボード	アラート	イベントとレポート	コンピュータ	ポリシー	
<ul> <li>□ □ □ イベント</li> <li>□ システムイベント</li> </ul>		レポートの生成			
□ ⑦ 不正ブログラム対	) 第イベント ■ンイベント イベント -				^
<ul> <li>         ○ (7) ショール     </li> <li>         ◎ (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4</li></ul>	*	<ul> <li>● マイエンピュータ</li> <li>○ グループ:</li> </ul>	14 Q		÷
▶ レポートの生成		01	[र	イコンピュータ	]を選択します。
		『暗号化			~
ĸ 🔯 1台のエンビュー	・タでセキュリティア・	ップデートを実行中			アラート 🔤 (0) 🔲 (1)

#### ⑧ 暗号化の設定をします。

	p Security				SPS123456789 ▼   ログオフ   @ ヘルプ ▼
ダッシュボード	7 <del>5</del> -ŀ	イベントとレポート	コンピュータ	ポリシー	
E 🏬 イベント		レポートの生成			
<ul> <li>□ システムイベント</li> <li>□ ② 不正プログラム対         ○ 隔離ファイル     </li> </ul>	策イベント	<b>単独レポート</b> 〇 コンピュータ:		[レポートノ	ペスワードの無効化]を選択します。
● WEDレビュナーショ ● ファイアウォールイ ● 役入防御イベント ● 変更監視イベント	ロンイベント	<ul> <li>暗号化</li> <li>● レポートのパスワードの</li> <li>● 現在のユーザのレオ</li> </ul>	<b>D無効化</b> トのバスフードを使用		
● セキュリティロラ法 ■ レポートの生成	·祝1ヘント	○ カスタムレポートのパフ パスワードの確認入力	Rワードの使用:  : 		 生成 ✓
«					アラート 🔤 (0) 🔲 (1)

#### ⑨ 設定が終わったら、レポートを生成します。

TREND. Deep Secu	ity		SPS123456789 ▼   ログオフ   🔞 ヘルプ ▼
ダッシュボード アラート	イベントとレポート <b>ゴビュー</b>	ターポリシー	
Image: Table T	レポートの生成		
<ul> <li>システムイベント</li> <li>マ 不正プログラム対策イベント</li> </ul>		5 <b>20</b> 5	
「福雄ファイル     「     「     「     「     「     「     、	0 コンピュータ: コンピュータ名		~
<ul> <li>◎ ファイアウォールイベン</li> <li>◎ (見入防御イベント</li> <li>◎ 変更監視イベント</li> </ul>	[生成]を·	クリックします。	
<ul> <li>         ・ セキュリティログ監視イベント         ・         ・         ・</li></ul>	<ul> <li>カスタムレポートのパスワードの使用:</li> <li>パスワードの確認入力:</li> </ul>		
			生成
«			アラート 🔤 (0) 🔲 (1)

#### 10 レポートが生成されます。

sps2.tayoreru.com から 推奨設定レポート.pdf (75.	9 KB)を開くか、または保存しますか? ×				
	ファイルを閉((O) 【保存(S) ▼ キャンセル(C)				
	レポートが生成されるとダウンロードの画面が表示されますので、 任意のフォルダに保存してください。				

# 4.タスクトレイアイコンについて

#### この章では、エージェントのタスクトレイアイコンについて説明します。

エージェント側でサーバプロテクションサービスのイベントを確認する場合、タスクトレイアイコンからクライアント用のコンソールを使用します。

# 4-1.イベントの参照

#### 4-1-1.クライアントの状態を確認する

① サーバプロテクションサービスのエージェントのタスクトレイを確認します。



② タスクトレイアイコンからクライアント用のコンソールを開きます。



③ クライアント用のコンソールが表示されます。



#### 4-1-2.クライアントのイベントを確認する

① 「4-1-1 クライアントの状態を確認する」の手順1~3でクライアント用のコンソールを開きます。

#### ② 通知の画面を開きます。

end Micro Deep Security	_	×
ent/07		
	宝行中	
不正プログラム対策		
ອີWebu⊁າ ສ∽≫ານ	42	
<ul> <li>ファイアウォール</li> </ul>		
● 侵入防御	444個のルール	
● 変更監視	保護できません	
😑 セキュリティログ監視	保護できません	
ポーネント		
不正プログラ	ムからの保護	
ウイルスパターンファイル	12.487.00	
ダメージクリーンナップテンプレート	1502	
許可アプリケーションリスト	1006	
IntelliTrap除外パターンファイル	1.285.00	
IntelliTrapパターンファイル	0.227.00	
スパイウェア監視パターンファイル	1.725.00	
スパイウェア /グレーウェアパターンファイル	17.25	
Aenisi年可いえ NR5 ーンファイル	1 456 00	[イベントの表示]をクリックします。
±n		
。 不正プログラムの検出時に通知(M)		
不正たWebのという 不正たWebのという		
8	イベントの表示[V]	]
	OK <b>キャンセル</b> 適用	

③ 各イベントのタブをクリックし、イベントの内容を確認します。



●MEMO ウイルス感染時の対処方法

「検索結果」に表示される処理が「駆除」、「削除」、「隔離」以外の場合、別途ウイルスの処理を行う必要があります。

**診照** 「「了 5. ウイルス感染時の対処方法



MEMO Webレピュテーションイベントの対処方法

特定の端末でエンドユーザ様に覚えのないWebサイトへのアクセスがブロックされたイベントが発生している場合は、その端末がウイルス感染している 可能性があります。調査をご要望の場合は弊社担当エンジニアまでご連絡ください。

# 5.ウイルス感染時の対処方法

この章では、予約検索やリアルタイム検索などでウイルスが検出された場合の対処を以下に記載します。

## 5-1.感染の確認

- ① 管理コンソールもしくはクライアントの[不正プログラム対策イベント]の画面で、「ウイルス名」と「処理」を確認します。
- ② 処理の欄で、「駆除」、「削除」、「隔離」以外が表示されていないかどうか確認します。 「駆除失敗」などが表示されている場合は、ウイルスに感染している可能性が高いと判断できます。

MEMO 「イベントの参照」方法は3-4-2、4-1-2をご確認下さい。

## 5-2.トレンドマイクロのホームページによるウイルス情報確認と削除

サーバプロテクションサービスではウイルス等の感染を検知すると自動的に駆除を試みます。 前セクションにて感染が確認された場合、以下の手順によりウイルスを駆除します。



ヒントゥイルス情報確認と削除方法

以下の操作は、「WORM\_STRATION.EV」というウイルスの対処を例にした作業例です。 なお、トレンドマイクロのホームページ上の操作は2016年5月時点での内容の為、内容が変っている可能性があることをご承知ください。

- 別のパソコンから、トレンドマイクロのホームページにアクセスします。 URL は、次の通りです。 <u>http://jp.trendmicro.com/jp/home/</u> 上記 URL より[セキュリティ情報]-[セキュリティデータベース]を開きます。
  - I.ホームページの中の「セキュリティデータベース」でウイルス情報を確認します。 「検索キーワードを入力」と書かれた入力域に、検出したウイルス名を入力し、右の「検索」をクリックします。



- Ⅱ. 検索結果から該当のウイルス情報を選択します。
  - ウイルスデータベース:検索結果が表示されます。該当のウイルス名をクリックします。

WORM_STRATION.CZ	検索
Threat Encyclopedia で「WORM_STRATION.CZ」を検索結果:1件	
検索結果の表示件数:1-1 WORM_STRATION.CZ dll shdo449BA67F.dll"作成活動ワームは、以下のファイルを作成します。%S \drpr449BA67F.	検索結果 10 V ystem%\shdo449BA67F.dll%System%

Ⅲ. ウイルス概要の確認ウイルスの概要が表示されます。



#### Ⅳ. 詳細内容の確認

 ページを下方向にスクロールして「詳細内容」を確認します。
 ここをクリックして詳細内容の[表示/非表示] を切り替えます
 アイルサイズ: 204,572 bytes
 タイブ: EXE
 タイブ: EXE
 メモリ常難: なし
 発見日: 2012年10月9日
 侵入方法
 ワームは、他のマルウェアに作成されるか、悪意あるWebサイトからユーザが誤ってダウンロードすることによりコン ビュータに侵入します。



#### Ⅵ. ウイルスを削除する。

「対応方法」のページに記載されている文章をよく読み、その手順に従ってウイルスを削除します。

この章では、管理コンソールに関する注意事項を記載します。

## 6-1.管理コンソールのエラー表示

管理コンソールの特定の項目を選択すると「このページは表示できません」というエラー画面が表示されます。これは、お客様の PC やネットワーク、また、サーバプロテクションサービスのシステム上の問題ではございませんのでご安心ください。

#### エラー画面を表示する項目

- ① [ポリシー]-[共通オブジェクト]-[その他]-[不正プログラム対策設定]
- ② [ポリシー]-[共通オブジェクト]-[リスト]- [ディレクトリリスト]
- ③ [ポリシー]-[共通オブジェクト]-[リスト]- [ファイルリスト]
- ④ [ポリシー]-[共通オブジェクト]-[リスト]- [ファイル拡張子リスト]

#### 以下に実際のエラー画面を掲載致します。



# 7.その他

この章では、お客様の環境変更などについての問い合わせ先を以下に記載します。

## 7-1.エージェントの追加

お客様が新たにサーバ購入された際や既存のサーバに対して当サービスでのセキュリティ対策をご希望される際は、担当営業かエンジニアまでご連絡ください。

# 7-2.サーバのリプレース

当サービスでご利用中のサーバをリプレースされる場合や廃棄される際は、担当営業かエンジニアまでご連絡ください。

### 7-3.設定の変更

当サービスでご利用中のサーバの設定変更をご希望される際は、「サーバプロテクションサービス登録完了のお知らせ」に記載されている連絡先までお問い合わせください。

- 以下の設定が変更可能となっています。
- ・推奨スキャン日時
- ・予約検索の有無
- •予約検索日時
- ・検索除外フォルダの指定

## 2017年 12月 1日 改訂

#### 本マニュアル内の記載内容を、無断で複写、記載することを禁じます

#### SPS-UM-F-20171201